Department of the Interior
Privacy Impact Assessment

September 8, 2014

Name of Project: Enterprise Data-at Rest (DAR) Encryption
Bureau: Office of the Secretary
Project's Unique ID: 010-000000666

Once the PIA is completed and the signature approval page is signed, please provide copies of the PIA to the following:

- Bureau/office IT Security Manager
- Bureau/office Privacy Act Officer
- DOI OCIO IT Portfolio Division
- DOI Privacy Act Officer

Do not email the approved PIA directly to the Office of Management and Budget email address identified on the Exhibit 300 form. One transmission will be sent by the OCIO Portfolio Management Division.

Also refer to the signature approval page at the end of this document.

A. CONTACT INFORMATION:

Teri Barnett
Departmental Privacy Officer
Office of the Chief Information Officer
U.S. Department of the Interior
1849 C Street, NW, Mail Stop 5547 MIB
Washington, DC 20240
202-208-1605

B. SYSTEM APPLICATION/GENERAL INFORMATION:

1) Does this system contain any information about individuals?

a. Is this information identifiable to the individual? *(If there is **NO** information collected, maintained, or used that is identifiable to the individual in the system, the remainder of the Privacy Impact Assessment does not have to be completed).*

Yes. The McAfee ePolicy Orchestrator (ePO) reporting server stores the employee's official username and the Endpoint Encryption Server stores the employees official username, first and last name. This information is downloaded from the Department of the Interior (DOI or Department) Active Directory (AD) Service.

b. Is the information about individual members of the public? *(If YES, a PIA must be submitted with the OMB Exhibit 300, and with the IT Security documentation).*

No, the information is about DOI employees and contractors.

c. Is the information about employees? (If yes and there is no information about members of the public, the PIA is required for the DOI IT Security C&A process, but is not required to be submitted with the OMB Exhibit 300 documentation).

Yes, the information is about DOI employees and contractors, and includes official username, and first and last name.

2) What is the purpose of the system/application?

The purpose of DOI's Enterprise Data-at-Rest (DAR) Encryption system is to improve information security within DOI by providing improved data encryption. This is achieved by using McAfee's Endpoint Encryption Protection (MEEP) server and McAfee's ePO to provide ongoing active encryption services that monitor, control and report the status of the encryption services performance as an ongoing service.

DOI's Enterprise DAR Encryption system consists of two major components, laptop endpoint encryption and endpoint encryption reporting. The laptop endpoint encryption component is managed by each DOI Bureau and the endpoint encryption reporting capability is centrally managed by the DOI Enterprise Services Branch, End User Services (EUS) Division within the Office of the Chief Information Officer (OCIO). The central and individual Bureau projects are coordinated by the DOI Project Management Office (PMO). When implemented and placed into production, DAR will be a distributed system managed and operated by the individual Bureaus and Offices with the central reporting component managed and operated by EUS Division. The Department will provide enterprise level oversight and compliance monitoring.

The central reporting ePO system instance will be owned and operated by OCIO-EUS Division with the purpose of the system and software to be a complete enterprise ePO instance for Department-wide collection and aggregation of information to meet DAR reporting needs including user-level configuration status reports pushed from the Bureaus, Department-wide encryption program status, and performance reporting between the Bureaus/Offices and Department including hardware, software, and telecommunications according to the system design and installation documents. The Endpoint Encryption servers will be owned and operated by each Bureau using MEEP server as a solution. The solution relies upon a deployed encryption agent to laptops running Windows operating systems within the respective Bureau. As appropriate and in accordance with Department and Bureau guidelines, laptops joined to the network are encrypted with McAfee Endpoint Encryption.

The DAR Assessment and Authorization (A&A) boundary includes the McAfee parent ePO application (server & Structured Query Language Database) and the McAfee Endpoint Encryption server application for all DOI Bureaus and Offices.

The EUS Division parent ePO server will reside in the Enterprise Hosting Center-West-Denver Federal Center campus, Lakewood, CO operations center. The child ePO servers and Bureau MEEP application servers will reside in the respective Bureau primary data center and backup locations. The locations include the following data center locations: Denver, CO; Reston, VA, Herndon, VA, Washington, DC; Boise, Idaho; Albuquerque, NM; and Arlington, VA.

OCIO-EUS Division currently has its offices in Reston, VA, which is where the parent ePO server reporting function is remotely managed and monitored.

3) What legal authority authorizes the purchase or development of this system/application?

The E-Government Act of 2002 (Pub. L. 107-347); DOI OCIO Directive 2001-004, Protecting Sensitive Data When Transferring, Donating, or Disposing of Computer Equipment; OMB M-06-15, Safeguarding Personally Identifiable Information; OMB M-06-16, Protection of Sensitive Agency Information; Departmental Regulations, 5 U.S.C. 301; Paperwork Reduction Act, 44 U.S.C. Chapter 35; Clinger-Cohen Act, 40 U.S.C. 11101, et seq.; OMB Circular A-130, Management of Federal Information Resources.

C. DATA in the SYSTEM:

1) What categories of individuals are covered in the system?

DOI employees and contractors with network account credentials are the only individuals covered in the system.

2) What are the sources of the information in the system?

a. Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?

The source of the information is the ePO system database and McAfee Endpoint Encryption servers.

b. What Federal agencies are providing data for use in the system?

DOI is the Federal agency providing data in the system. No other Federal agency provides data for use in this system.

c. What Tribal, state and local agencies are providing data for use in the system?

No Tribal, state or local agencies are providing data for use in this system.

d. From what other third party sources will data be collected?

There are no other third party sources that provide data for this system.

e. What information will be collected from the employee and the public?

No data will be collected directly from the employee or from the public. DOI employees' and contractors' usernames, first and last names are retrieved from DOI's Active Directory.

Additional information collected are encryption keys, recovery information, secure server keys and the following machine information: computer hostname, domain name, fully qualified domain name, unique machine identification tag, McAfee ePO integrated products and version installed, date and time stamp for product updates, IP address, IP version, subnet mask, network address, operating system, OS Version, time zone and system description.

3) Accuracy, Timeliness, and Reliability

a. How will data collected from sources other than DOI records be verified for accuracy?

N/A. No data will be collected from non-DOI sources.

b. How will data be checked for completeness?

The data being reported is the encryption status of the Departmental laptops which is reported through ePO. The initial deployment of the parent ePO reporting server included requesting the number of laptops from each Bureau or Office based on their laptop inventory. This number was then compared with the number of laptops that were reporting from the child ePO servers to the parent ePO server for verification for accuracy.

Going forward the McAfee ePO server maintains trending data that is used to detect a drastic change in the quantity of laptops. The trending data is manually monitored by the ePO administrator on a daily basis. If any anomalies are determined, then the parent ePO administrator troubleshoots with the child ePO administrator to resolve the issue, including identifying the source of the issue to ensure it is not repeated.

c. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).

Yes, the data is current and is pulled weekly from the child ePO servers to ensure it is not out-of-date. The McAfee Endpoint Encryption and ePO user guides provide details of this configuration.

The Bureau ePO servers residing on the networks external from the parent ePO server are responsible for manually emailing the reports via the DOI email system on a monthly basis. Locally, the data is updated daily.

d. Are the data elements described in detail and documented? If yes, what is the name of the document?

DAR System Security Plan, May 30, 2014

DAR Assessment and Authorization Approval, May 02, 2014

OCIO Directive 2010-004, The Department of the Interior (DOI) Enterprise Data-at-Rest (DAR) Encryption Initiative, February 5, 2010

D. ATTRIBUTES OF THE DATA:

1) Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

Yes. The use of the data is relevant and necessary for the purpose of encrypting and monitoring the encryption status of laptops at the DOI to verify compliance. McAfee products are commercial off the shelf (COTS) implementation that do not allow for customization of their database fields.

2) Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?

No. The purpose of the system is to encrypt and monitor the encryption status of laptops at DOI to verify compliance. The system will neither derive new data nor create previously unavailable data about an individual through aggregation.

3) Will the new data be placed in the individual's record?

No. The system does not derive new data about individuals or place data in individuals' records.

4) Can the system make determinations about employees/public that would not be possible without the new data?

No. The system does not derive new data or make determinations about employees or members of the public.

5) **How will the new data be verified for relevance and accuracy?**

   Not applicable. The system does not derive new data about individuals.

6) **If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?**

   Not applicable. Data is not being consolidated.

7) **If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access?** Explain.

   Not applicable. Processes are not being consolidated.

8) **How will the data be retrieved? Does a personal identifier retrieve the data?** If yes, explain and list the identifiers that will be used to retrieve information on the individual.

   No, data is not retrieved by use of a personal identifier. Retrieval of data within the ePO server is completed by searching for machine name.

9) **What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?**

   Only authorized OCIO-EUS Division and system administrators will have access to the ePO system and Endpoint Encryption server. The reports that will be produced will be aggregate reports for status of laptop encryption compliance and monitoring. Reports will not be produced on individual employees.

10) **What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent.)**

    No data will be collected directly from individuals, so there is no opportunity for individuals to decline or consent to the use of information. DOI employees' and contractors' usernames, first and last names are retrieved from DOI's Active Directory for use in the system. DAR is a Department-wide mandate and employees must adhere to the DOI Rules of Behavior governing the use of DOI information resources and data handling procedures prior to accessing DOI networks or systems.

E. MAINTENANCE AND ADMINISTRATIVE CONTROLS:

1) **If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?**

The EUS Division parent ePO server will reside in the Enterprise Hosting Center-West-Denver Federal Center campus, Lakewood, CO operations center. The child ePO servers and Bureau McAfee EEPC application servers will reside in the respective Bureau primary data center's location: Denver, CO; Reston, VA; Herndon, VA; Washington, DC; Boise, Idaho; Albuquerque, NM; and Arlington, VA. OCIO-EUS Division currently has its offices in Reston, VA, which is where the parent ePO server reporting function is remotely managed and monitored.

The system installation guides detail the system configuration, and once the systems are configured other than for routine maintenance the systems are not modified without a request for change being submitted to the systems change advisory board (CAB). The information contained in the parent ePO server is the laptop encryption status report for the DOI. This data is not locally generated, but a report is generated based on the information received from the Bureau (child) ePO servers. The information is pulled weekly from all ePO servers connected to the same network as the parent ePO server to ensure consistency for all sites.

The ePO servers residing on networks external from the parent ePO server are responsible for manually emailing the reports via the DOI email system on a monthly basis. Locally, the data is updated daily.

2) What are the retention periods of data in this system?

The disposition is Temporary. Data contained in this system is cut off when employee or contractor user accounts are terminated, and destroyed after one year in accordance with the Office of the Secretary Records Schedule 1404.3 User identification files (Routine systems).

3) What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?

Records on electronic media are degaussed and paper records are disposed of by shredding, in accordance with records disposition procedures outlined in 384 Department Manual 1.

4) Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?

No, the system is not using technologies in ways that DOI has not previously employed. The intent of the system is to protect the confidentiality of data at rest and provide an encryption status report on an enterprise level.

5) How does the use of this technology affect public/employee privacy?

The system is only used internally within DOI to encrypt and monitor the encryption status of Departmental computer systems and has only a minimal affect on employee privacy. This affect is mitigated by the fact that the system encrypts DOI computer systems in an effort to safeguard DOI information assets and protects individual privacy. The use of this technology does not affect public privacy because it is used internally within DOI.

6) **Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.**

No, the system will not provide the capability to actively monitor individuals. The system user's Enterprise AD username to identify and maintain the encryption status of the user's laptop. However, the system does not have the capability to locate and monitor the user or user's system activity.

7) **What kinds of information are collected as a function of the monitoring of individuals?**

The system will not provide the capability to monitor individuals, it only identifies the encryption status of an employee's computer.

8) **What controls will be used to prevent unauthorized monitoring?**

Numerous system access controls are in place to prevent unauthorized monitoring. Such controls include username and password authentication to access the servers. Physical security, including door locks requiring access card or keyed entry for authentication. Video camera surveillance and physical security guards at the data centers housing the servers are also in place in accordance with the NIST SP 800-53 security requirements. The systems are also behind firewalls, have their audit logs periodically reviewed, and audit logs automated alerts triggered when an anomaly occurs.

9) **Under which Privacy Act systems of records notice does the system operate? Provide number and name.**

Not applicable — This is not a Privacy Act System of records.

10) **If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.**

Not applicable – This is not a Privacy Act System of records.

F. ACCESS TO DATA:

1) **Who will have access to the data in the system?** (E.g., contractors, users, managers, system administrators, developers, tribes, other)

System administrators (SA) will have access to the data in the system. This access is granted based on least-privilege and assigned within the application. The SA's are DOI employees including contractor employees who are designated administrators.

2) **How is access to the data by a user determined?** Are criteria, procedures, controls, and responsibilities regarding access documented?

   User access is based on the principle of least privilege. Requests for Change (RFC) must be completed and approved prior to being granted access to the system. The CAB approves/disapproves the RFC based on the board's determination of need.

3) **Will users have access to all data in the system or will the user's access be restricted? Explain.**

   There are different access levels. As such not all users will have access to all data. The majority of users will have access to a subset of data. Only SAs, program leads, and the Chief Information Security Officer (CISO) will have full access.

4) **What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access?** (Please list processes and training materials)

   Access control via AD for network authentifation and the authentication required to log in to the ePO server are in place to prevent the misuse of data. Authorized users must agree to systems rules of behavior. Mandatory security and privacy training, audit logs and reviews are also controls that are in place to prevent the misuse of data by those having access.

5) **Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system**? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed?

   Contractors are involved with the design and development of the system and Privacy Act contract clauses are inserted in their contracts.

6) **Do other systems share data or have access to the data in the system? If yes, explain.**

   No. Other systems do not have access to the data nor does the system share the data to other systems. The system receives data from Active Directory however, this is a one way pull and the information is not returned.

7) **Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**

   The CISO, ESN Systems Manager, and the System Owner are responsible for protecting the privacy rights of the public and employees affected by the interface.

8) Will other agencies share data or have access to the data in this system (Federal, State, Local, Other (e.g., Tribal))?

No other agency will have access to the data in the system.

9) How will the data be used by the other agency?

No other agency will have access to the data in the system.

10) Who is responsible for assuring proper use of the data?

The OCIO-EUS Division IT Security manager is responsible for assuring the proper use of data.